BLACK CELL
Protecting critical infrastructures

Overview on VMware ESXi vulnerability CVE-2021-21974

Vulnerability affecting VMware ESXi hypervisors

CVE-2021-21974

A new vulnerability was reported by security researchers. This article describes an explosion in the compromises of VMware ESXi hypervisors with over 500 machines hit by ransomware this weekend, with the automated attacks likely exploiting CVE-2021-21974.

VMware initially described CVE-2021-21974 (CVSS 8.8 [HIGH]) in its February 2021 VMSA-2021-0002 advisory as letting a "malicious actor residing within the same network segment as ESXi who has access to port 427 may be able to trigger the heap-overflow issue in OpenSLP service resulting in remote code execution".

The implementation VMware is based on OpenSLP 1.0.1. VMware maintains its own version and has added hardening to it. The service parses network input without authentication and runs as root, so a vulnerability in the ESXi SLP service may lead to pre-auth remote code execution as root. This vector could also be used as a virtual machine escape, since by default a guest can access the SLP service on the host.

It seems there is a new type of malware and by its repertoire it can be useful for threat actors to exploit this vulnerability and gain unauthorized access to the system. This ransomware encrypts files with the .vmxf, .vmx, .vmdk, .vmsd, and .nvram extensions on compromised ESXi servers and creates a .args file for each encrypted document with metadata. Victims have also found ransom notes named "ransom.html" and "How to Restore Your Files.html" on locked systems. Other victims claimed their notes being plaintext files. Paying the ransom demanded by attackers is ill advised for several reasons, including encouraging the attackers to continue or even escalate their malicious activities, as they know that there is a profitable market for their actions; and there is no guarantee that paying the ransom will result in the attacker providing the decryption key or unlocking the affected files. Also, by paying the ransom, you may be indirectly funding illegal and unethical activities, such as the development and distribution of malware.

After this vulnerability, ESXi servers are more popular in the black market than ever, and several threat actor groups were looking for a vulnerability of ESXi servers. That's why we would like to introduce this vulnerability and give you some advice how to harden your system to increase its resilience against this attack vector.

First you should check your system configuration and review your currently used security solutions and if you find an ESXi server which is unpatched, then make sure the server is protected with a firewall, with no ports exposed. VMware's earlier

mitigation for the vulnerability urged users to 1: Login to the ESXi hosts using an SSH session (such as putty); 2: Stop the SLP service on the ESXi host with this command: */etc/init.d/slpd stop* (nb The SLP service can only be stopped when the service is not in use; users can check the operational state of SLP Daemon: *esxcli system slp stats get* 3: Run this command to disable the service: *esxcli network firewall ruleset set -r CIMSLP -e 0*

For Bare Metal customers using ESXi we strongly recommend in emergency :

- to deactivate the OpenSLP service on the server or to restrict access to only trusted IP addresses (https://kb.vmware.com/s/article/76372)
- to upgrade you ESXi on the latest security patch

After the these steps we recommend to ensure:

- your critical data is backed up (on immutable storage?),
- only necessary services are active and filtered with ACL to only trusted IP addresses,
- monitor your system for any abnormal behaviour.

With these steps you will be able to make your system more resistant against threat actor groups and other malicious activities which would like to exploit this vulnerability on your system.

Sources: [date of access: 10.02.2023]

BleepingComputer (https://www.bleepingcomputer.com/news/security/massive-esxiargs-ransomware-attack-targets-vmware-esxi-servers-worldwide/)

VMware (https://www.vmware.com/security/advisories.html)

TechCrunch (https://techcrunch.com/2023/02/06/hackers-vmware-esxi-ransomware)

Varonis (https://www.varonis.com/blog/vmware-esxi-in-the-line-of-ransomware-fire)